CA Nimsoft Monitor para Flow Analysis

Guía del usuario

Versión 1.0

Historial de revisiones del documento

Versión del documento	Fecha	Cambios
1.0	9/10/2012	Versión inicial de la *Guía del usuario de CA Nimsoft Monitor para Flow Analysis*

Contacto con Nimsoft

Para su conveniencia, Nimsoft proporciona un sitio en el que se puede acceder a la información que necesita acerca de los productos de Nimsoft.

Desde la página http://support.nimsoft.com/, se puede acceder a lo siguiente:

- Información para el contacto telefónico y en línea para poder acceder a los servicios de atención al cliente y de asistencia técnica
- Información sobre foros y comunidades de usuarios
- Descargas de documentación y productos
- Directrices y políticas de soporte de Nimsoft
- Otros recursos útiles adecuados para el producto

Comentarios

Si tiene comentarios o preguntas sobre la documentación de productos de Nimsoft, puede enviar un mensaje a support@nimsoft.com.

Avisos legales

Copyright © 2012, CA. All rights reserved.

Garantía

El material incluido en este documento se proporciona "tal cual" y es sujeto a sufrir modificaciones, sin previo aviso, en ediciones futuras. En la medida que lo permita la legislación aplicable, Nimsoft LLC no da ningún tipo de garantías, ya sean explícitas o implícitas, con respecto a este manual y cualquier tipo de información contenida en el presente, incluyendo, sin limitación, las garantías implícitas de comercialidad y de adecuación para un fin específico. Nimsoft LLC no se hará responsable de los errores o los daños incidentales o consecuenciales derivados del suministro, uso o desempeño de esta documentación o de cualquier otra información contenida en la presente. En el caso de que Nimsoft LLC y el usuario tengan un acuerdo por escrito independiente sobre los términos de garantía cubriendo el material contenido en la presente que entre en conflicto con los presentes términos, los términos de garantía del acuerdo independiente son los que regirán.

Licencias de tecnología

El hardware y/o software que se describe en esta documentación están suministrados bajo una licencia y únicamente se pueden utilizar o copiar en conformidad con los términos de dicha licencia.

No se puede reproducir ninguna parte de este manual de ninguna manera ni por ningún medio (incluido el almacenamiento electrónico y la recuperación o traducción a un idioma extranjero) sin consentimiento por escrito ni acuerdo previo por parte de Nimsoft LLC, tal y como rigen las leyes de copyright internacionales y de Estados Unidos.

Leyenda de derechos restringidos

Si el software está dirigido al uso del gobierno de Estados Unidos, al desempeñar un contrato o subcontrato principal, el software se entrega y se autoriza como "Software de equipo comercial", tal y como se ha definido en DFAR 252.227-7014 (junio 1995); o como un "elemento comercial", en FAR 2.101 (a); o como "Software de equipo restringido", en FAR 52.227-19 (junio 1987); u otro tipo de regulación de agencia equivalente o cláusula de contrato. El uso, la duplicación o la revelación del software se rige por los términos de licencia comerciales y estándares de Nimsoft LLC. Los departamentos y agencias del gobierno de Estados Unidos no recibirán más derechos a parte de los Derechos restringidos que se han definido en FAR 52.227-19(c)(1-2) (junio 1987). Los usuarios del gobierno de EE. UU. no recibirán más que los Derechos restringidos, tal y como se ha definido en FAR 52.227-14 (junio 1987) o en DFAR 252.227-7015 (b)(2) (noviembre 1995), según corresponda en los datos técnicos.

Marcas comerciales

Nimsoft es una marca comercial de CA.

Adobe®, Acrobat®, Acrobat Reader® y Acrobat Exchange® son marcas comerciales registradas de Adobe Systems Incorporated.

Intel® y Pentium® son marcas comerciales registradas en Estados Unidos de Intel Corporation.

Java(TM) es una marca comercial de EE. UU. de Sun Microsystems, Inc.

Microsoft® y Windows® son marcas comerciales registradas de EE. UU. de Microsoft Corporation.

Netscape(TM) es una marca comercial de EE. UU. de Netscape Communications Corporation.

Oracle® es una marca comercial registrada de EE. UU. de Oracle Corporation, Redwood City, California.

UNIX® es una marca comercial registrada de Open Group.

ITIL® es una marca registrada de Office of Government Commerce (OGC, Oficina de Comercio Gubernamental) en el Reino Unido y otros países.

Todas las demás marcas comerciales, nombres comerciales, marcas de servicio y logotipos a los que se hace referencia aquí pertenecen a sus empresas respectivas.

Contenido

Capítulo 1: Introducción 7

Acerca de esta guía 7
Conceptos de Flow Analysis 8
Terminología de Flow Analysis 8

Capítulo 2: Procedimientos iniciales 11

Requisitos previos 11
Implementación del portlet Flow Analysis Reporter 12
Configuración 16
Apertura del puerto 9995 (UDP) 17
Dispositivos de red 17
Apertura de la interfaz gráfica de usuario de la configuración 19
Configuración de la sonda de Flow Analysis 20
Configuración de Flow Analysis Collector 21
Configuración de los informes 27

Capítulo 3: Informes 29

Generación de informes de datos de Flow Analysis 29
Elementos comunes 29
Elementos de la barra superior 29
Opciones para el gráfico 30
Opciones para la vista de columna 31
Arrastre de columnas 31
Vínculos para la obtención de detalles 31
Visualización de la información sobre herramientas 32
Cadena de información 32
Ventana principal 32
Interfaces 34
Hosts 36
Aplicación 37

Capítulo 4: Solución de problemas 39

No se muestran datos en los informes (retraso del tiempo de los datos del informe) 39

No funcionan los vínculos a USM 40
El vínculo a USM muestra un dispositivo incorrecto 41
No se muestra el recopilador en el menú desplegable 41
Interfaz denominada Null0 o Nu0 42
Código de mensaje de error 500 42
Código de mensaje de error 400 42
Código de mensaje de error 200 43

Capítulo 1: Introducción

Acerca de esta guía

Esta guía le ayuda a obtener el máximo de la solución CA Nimsoft Monitor para Flow Analysis. Contiene las secciones siguientes:

- **Introducción**: Información acerca de esta guía y una introducción a los conceptos de Flow Analysis
- **Procedimientos iniciales**: Pasos necesarios para empezar a utilizar Flow Analysis
  - Componentes de los requisitos previos
  - Configuración del portlet Reporter
  - Configuración: Tareas de configuración necesarias para:
    - el acceso de puertos y los enrutadores que proporcionan datos del flujo de red
    - la sonda Flow Analysis y el sistema del recopilador
    - el portlet y la GUI de Flow Analysis
- **Informes**: describe la GUI de Flow Analysis, sus controles y los informes de datos del flujo que están disponibles
- **Solución de problemas**: describe problemas de uso del producto y sus soluciones.

Conceptos de Flow Analysis

Flow Analysis se ha diseñado para integrar una vista del tráfico que fluye por la red con datos de la calidad del servicio y alarmas. Esta vista es completamente visible en Nimsoft Unified Management Portal (UMP). Con Flow Analysis, se puede:

- Identificar inmediatamente las interfaces, los host y las aplicaciones que generan la mayor parte del tráfico de su empresa. Esta información es esencial para la solución de problemas a corto y largo plazo.
- Revisar las alarmas de Nimsoft juntamente con los datos del flujo para poder identificar los problemas de red rápidamente.
- Analizar las tendencias en aplicaciones, host y conversaciones por clases de servicios. Esta información le ayuda a optimizar la infraestructura de la red para el rendimiento de la aplicación.

Terminología de Flow Analysis

NetFlow

NetFlow hace referencia a los protocolos (NetFlow versiones 5, 7 y 9, así como IPFIX, Jflow, sFlow, cflowd, Rflow y NetStream) que permiten la recopilación de estadísticas de tráfico de IP en interfaces de dispositivos de red. Un enrutador se configura para exportar información del flujo, enviando paquetes de UDP que contienen estadísticas del flujo a un recopilador.

La información del flujo es útil al responder las siguientes preguntas:

- ¿Conoce todas las aplicaciones que se ejecutan en la red?
- ¿Qué patrones de tráfico de las aplicaciones se muestran?
- ¿Qué aplicaciones y host están consumiendo la mayor parte de la banda ancha?
- ¿Cuánta capacidad de vínculo se necesita en el futuro? ¿Realmente la solución a los problemas de rendimiento es tener más banda ancha?

Conversación

Una conversación es una sesión de tráfico de subred a subred o de usuario a usuario (host a host). El portal de Flow Analysis muestra esta información: por ejemplo, se puede descubrir si una conversación determinada está causando un pico de tráfico en una interfaz y se pueden identificar las principales conversaciones basadas en el volumen.

Flujo

Un flujo es un conjunto de paquetes de IP que pasan un punto de observación de la red durante un cierto intervalo de hora. Un flujo puede estar formado por Flexible NetFlow, Sampled NetFlow, NetFlow v5, v7 o v9; sFlow versión 5 o cualquier otra versión similar de IPFIX, Jflow, cFlow o NetStream.

Interfaz

Una interfaz es un punto de conexión, como un número de serie, Frame Relay, Fast Ethernet, ATM o una interfaz PVC. Flow Analysis informa sobre cualquier interfaz lógica que se activa en un enrutador compatible que tiene activado el flujo. El portal muestra las interfaces que se monitorizan en el entorno.

Protocolo

Un protocolo es un estándar para regular la comunicación entre equipos. Los protocolos comunes incluyen: HTTP, SNMP, FTP y VoIP. La información que se muestra puede incluir los principales protocolos entrantes y salientes de una determinada interfaz. Esta información le puede ayudar a identificar qué aplicación está causando tráfico de red. También se pueden crear y ejecutar informes para determinar qué protocolos y aplicaciones utilizan los diferentes grupos de la organización.

Calidad del servicio

La calidad de servicio es un nivel definido de rendimiento en una red de datos, es decir, la calidad de transmisión y disponibilidad de los servicios.

Informe

Un informe es una visualización de datos recopilados que se pueden consultar en el portlet de Flow Analysis en UMP. Se pueden exportar informes como archivos separados por comas (CSV).

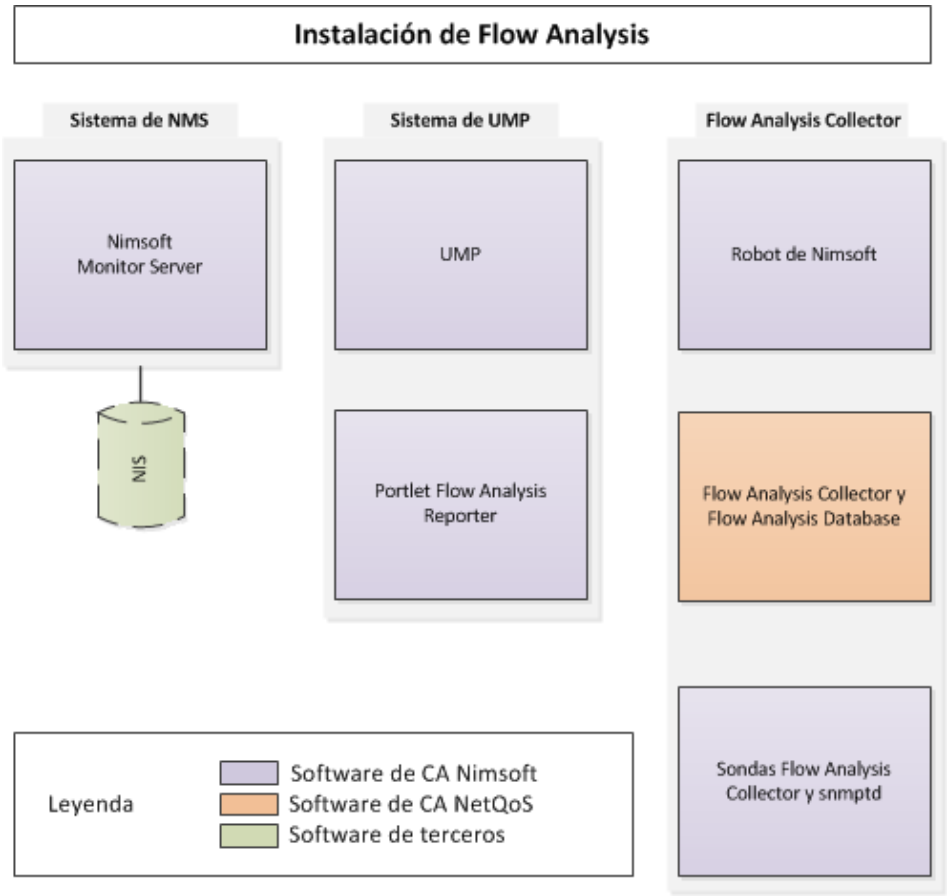
Capítulo 2: Procedimientos iniciales

Esta sección contiene los siguientes temas:

Requisitos previos (en la página 11)
Implementación del portlet Flow Analysis Reporter (en la página 12)
Configuración (en la página 16)

Requisitos previos

Consulte la *Guía de instalación de Flow Analysis* y confirme que todos los componentes de software necesarios están instalados, bajo licencia y operativos:



- Nimsoft Monitor Server y base de datos de NIS
- Unified Monitoring Portal (UMP) y el portlet Flow Analysis Reporter
- Flow Analysis Collector, Flow Analysis Database, un robot de Nimsoft, la sonda Flow Analysis Collector y la sonda snmptd.

Nota: Flow Analysis Collector y Flow Analysis Database se basan en los productos CA NetQoS Harvester y Reporter/Analyzer, respectivamente.

Implementación del portlet Flow Analysis Reporter

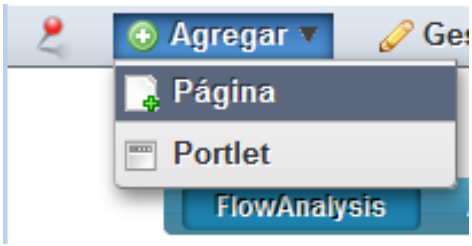
Para configurar los componentes de Flow Analysis y consultar los informes de los datos de flujo, se debe implementar el portlet Flow Analysis Reporter dentro de Unified Monitoring Portal (UMP).

Siga estos pasos de los procedimientos iniciales:

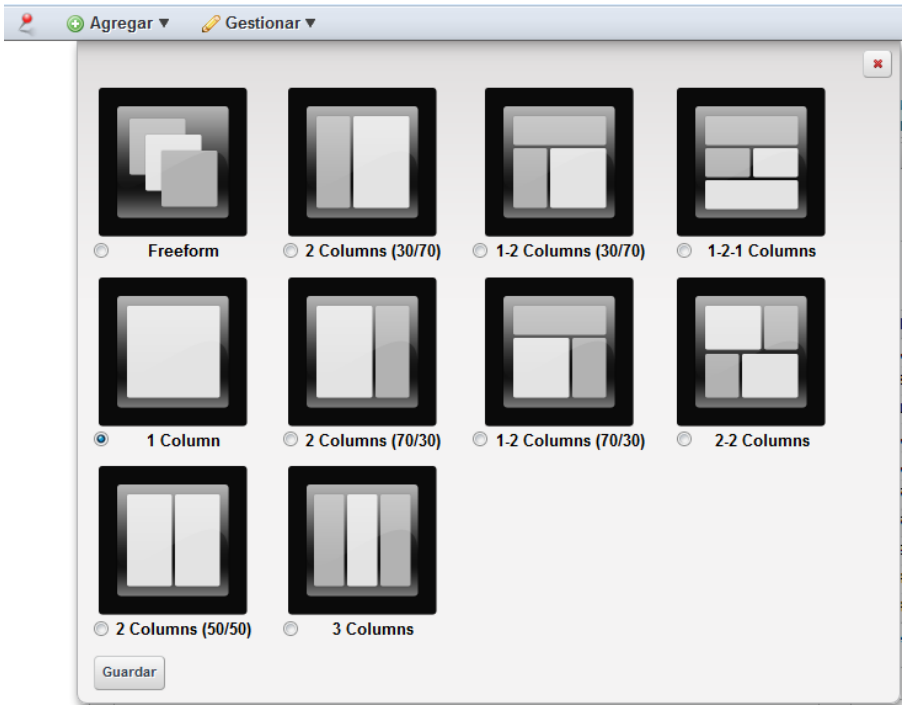
1. Confirme que la sonda ump_flow se ha implementado en el robot del sistema de UMP. Se puede comprobar en el Gestor de la infraestructura. Busque el icono del robot del sistema de UMP. El icono de la sonda ump_flow se muestra debajo del mismo y debe estar de color verde. Para revisar las instrucciones de la instalación, consulte la sección Instalación del portlet Flow Analysis Reporter de la *Guía de instalación de Flow Analysis*).
2. Inicie UMP (http://<direcciónIP_sistema_UMP>)
3. Siga los pasos que se muestran a continuación para agregar la ficha Flow Analysis a UMP.

   Nota: Un tratamiento más completo para configurar de páginas y portales dentro de UMP está disponible en la ayuda en línea de UMP en la sección **Bienvenida > Procedimientos iniciales con UMP**.

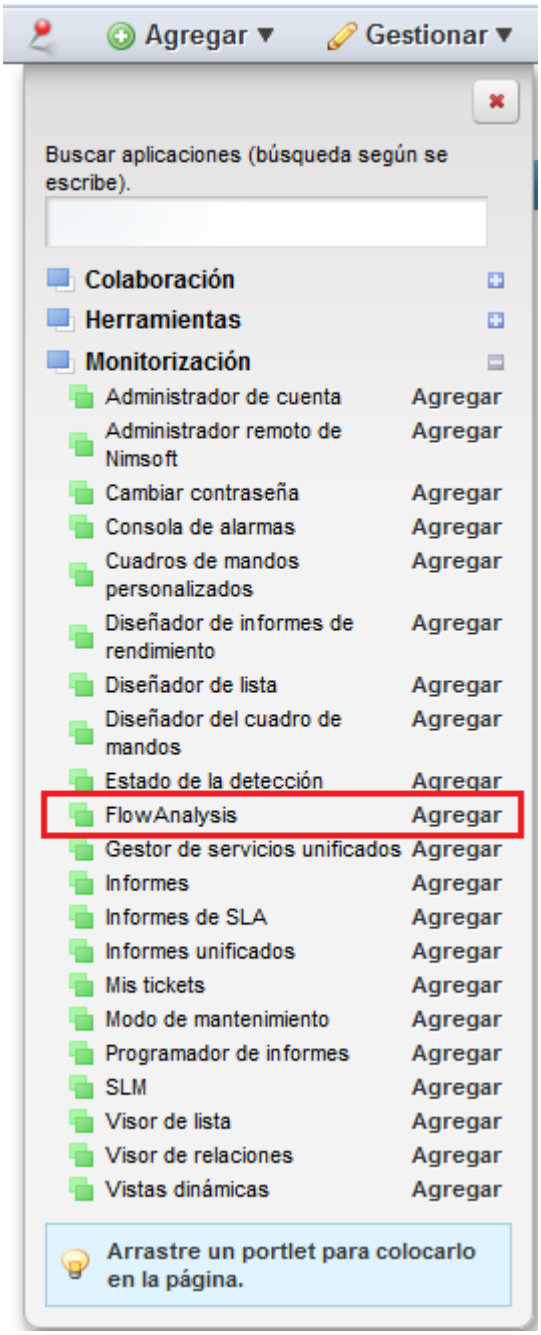
   1. Agregue una página vacía: En la parte izquierda superior de UMP, elija: **Agregar > Página,** asigne un nombre a la página nueva (recomendamos "Flow Analysis") y, a continuación, haga clic en la marca de verificación para confirmar y guardar.



2. Ajuste el diseño de la página: Seleccione la página nueva y, a continuación, seleccione **Gestionar > Diseño de la página > Columna 1** en el menú de la parte superior izquierda de la ventana del explorador y seleccione **Guardar**.



3. Instale el portlet de Flow Analysis en la página nueva: Elija **Agregar > Portlet.** A continuación, seleccione Flow Analysis bajo **Monitorizar** y haga clic en **Agregar.**



4. El portlet se carga en la página, se inicia y encuentra recopiladores disponibles de Flow Analysis. Los que se encuentran se muestran en la lista desplegable Recopiladores en el formulario "concentrador/robot/dominio."

Nota: La sonda discovery_server debe estar en ejecución en el host de NMS para que la lista desplegable Recopiladores muestre los recopiladores de Flow Analysis. Es posible que, si un recopilador existente no se enumera en este menú desplegable, no se haya detectado todavía. Si se reinician las sondas discovery_server y discovery_agent, la detección se volverá a ejecutar y se encontrarán más recopiladores.

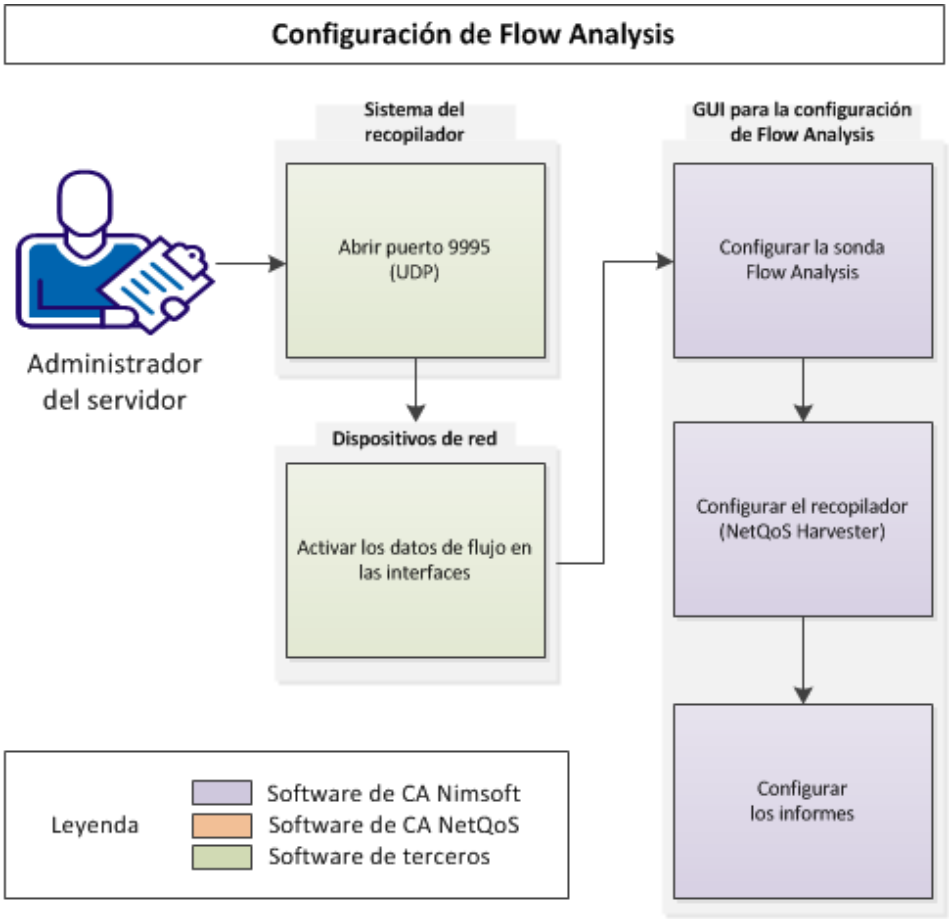
5. Seleccione el recopilador deseado en la lista desplegable.
6. La página principal de Flow Analysis muestra estos tres gráficos de los principales X datos de generación de informes:
    1. Interfaces principales
    2. Host principales
    3. Aplicaciones principales.

Nota: Es posible que, si se acaba de iniciar el sistema, los datos no se vean hasta que haya pasado un intervalo de quince minutos.

Se pueden obtener más detalles de los datos mostrados haciendo clic en los vínculos azules. Consulte la sección Página principal de Flow Analysis (en la página 32) para obtener más detalles.

Configuración

La configuración de Flow Analysis está formada por las tareas siguientes:


Configuración de Flow Analysis
Sistema del recopilador
GUI para la configuración de Flow Analysis
Abrir puerto 9995 (UDP)
Configurar la sonda Flow Analysis
Administrador del servidor
Dispositivos de red
Activar los datos de flujo en las interfaces
Configurar el recopilador (NetQoS Harvester)
Configurar los informes
Leyenda
Software de CA Nimsoft
Software de CA NetQoS
Software de terceros

Un administrador del sistema con conocimientos sobre Windows Server 2008 y derechos administrativos completos sobre los host realiza estos pasos de la configuración:

1. Abre el puerto 9995 para el tráfico de UDP en el sistema de Flow Analysis Collector.
2. Activa NetFlow (u otro protocolo de monitorización de flujo) en interfaces de dispositivos de red (es posible que sea necesario un administrador de red con el acceso administrativo a estos dispositivos para realizar este paso).
3. Configura la sonda Flow Analysis.
4. Configura Flow Analysis Collector.
5. Configura los informes.

Apertura del puerto 9995 (UDP)

Abra el puerto 9995 para el tráfico de UDP en el host del recopilador. Confirme que el tráfico de UDP puede pasar por los dispositivos de red y por el host del recopilador mediante este puerto.

Dispositivos de red

Para activar NetFlow en los enrutadores compatibles con NetFlow, complete los pasos siguientes en los enrutadores compatibles con las versiones 5, 7 o 9 de NetFlow.

Nota: Antes de empezar, recopile la información siguiente para los enrutadores que planea monitorizar:

- Dirección de la fuente
- Cadena de comunidad de lectura de SNMP
- Versión de NetFlow (si se aplica)

Protocolos de flujo compatibles:

- NetFlow v5, v7 y v9
- sFlow versión 5
- IPFIX, Jflow, cFlow y estándares de NetStream que cumplen los estándares de NetFlow v5, v7 o v9

Siga estos pasos:

1. Guarde una copia de seguridad de la configuración actual en el escritorio o en un servidor de protocolo trivial de transferencia de archivos (TFTP).
2. Ejecute el comando **copy run start** o **wr mem** antes de realizar cualquier cambio en los enrutadores que desea monitorizar.

   La ejecución de este comando permite garantizar que todas las configuraciones actuales se guardan en una memoria estática en el caso de que el enrutador se bloquee o se vuelva a iniciar.
3. Configure la exportación de NetFlow introduciendo los comandos de IOS siguientes en este orden:

   ```
   ip flow-export version <número_versión>
   ip flow-export source <interfaz>
   ip flow-export destination <direcciónIPsistemainstalación> 9995
   ip flow-cache timeout active 1
   ```

   Nota: Para el segundo comando de la serie, puede modificarse la dirección IP de la interfaz de la fuente. Cisco recomienda la configuración de una interfaz de fuente de bucle.
4. Para cada interfaz lógica, vaya a la interfaz e introduzca:
   ```
   ip route-cache flow
   ```

   o
   ```
   ip flow ingress (para nuevas versiones de IOS)
   ```
5. Configure la persistencia del índice en cada enrutador mediante el comando siguiente:
   ```
   config# snmp-server ifindex persist
   ```

   Nota: Los enrutadores de la familia Cisco 7200 Series, 7500 Series y 12000 GSR son compatibles con la persistencia del índice.
6. Si utiliza los conmutadores Catalyst 6500 o 7600, verifique que tiene un motor de supervisión Sup II o superior.

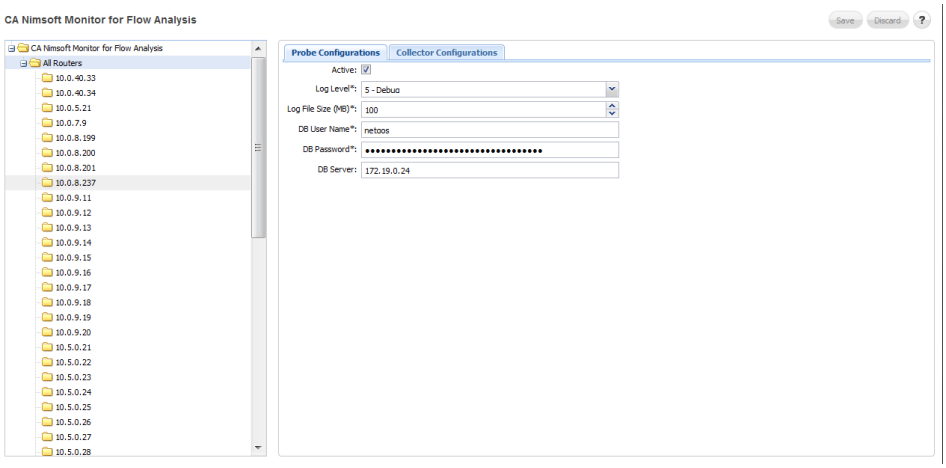
   Nota: Para el resto de comandos de los enrutadores Catalyst 6500 y 7600, consulte la documentación acerca de los comandos de NetFlow de Cisco.

Verifique que se hayan recibido los datos de flujo.

En el sistema del recopilador (donde está instalado el componente de software de Flow Analysis Database), vaya al directorio D:\NETQOS\Netflow\datafiles\HarvesterWork. Debería haber varios archivos en este directorio con el nombre <valor_numérico>-9995.tbn.inc. Es posible que también hayan otros archivos con el mismo esquema de denominación pero con la extensión de archivo .tmp. Si existen archivos <valor_numérico>-9995.tbn.inc que tienen más de 0 KB, significa que se han recibido los datos de flujo.

Apertura de la interfaz gráfica de usuario de la configuración

Haga clic en el botón **Configure** (Configurar) que se encuentra en la parte superior derecha de la interfaz gráfica de usuario de Flow Analysis en UMP para abrir la interfaz gráfica de usuario de configuración en una ventana separada:

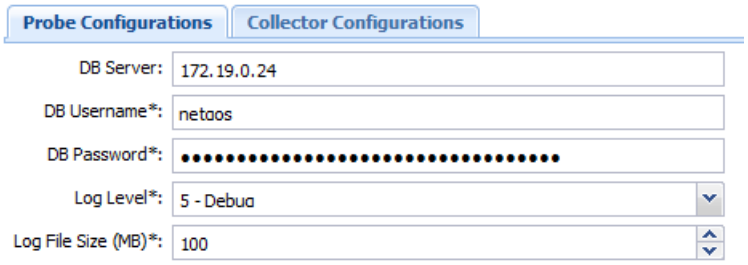


Cuando se inicia la GUI de configuración por primera vez, no se muestran datos en el marco izquierdo hasta que se activa un recopilador. Cuando se activa un recopilador, se muestra la jerarquía de los dispositivos de red.

En el marco derecho aparecen las fichas **Probe Configurations** (Configuraciones de la sonda) y **Collector Configurations** (Configuraciones del recopilador) que controlan los valores de configuración de la sonda y del recopilador de Flow Analysis respectivamente.

Configuración de la sonda de Flow Analysis

La ficha Probe Configurations (Configuraciones de la sonda) de la interfaz gráfica de usuario para la configuración de Flow Analysis permite establecer y cambiar los atributos siguientes:



Atributo	Tipo	Notas
DB Server (Servidor de la base de datos)	Dirección IP	IP de Flow Analysis Database
DB Username (Nombre de usuario de la base de datos)	Cadena	Nombre de usuario para Flow Analysis Database; valor predeterminado = "netqos"
DB Password (Contraseña de la base de datos)	Cadena	Valor predeterminado = "netqos"
Log Level (Nivel del registro)	Número entero (1-5)	0=Apagado, 1=Gravedad, 2=Error, 3=Advertencia, 4=Información y 5=Depuración
Log File Size (MB) (Tamaño del archivo de registro en MB)	Número entero (1-1000)	

Configuración de Flow Analysis Collector

En la ficha **Collector Configurations** (Configuraciones del recopilador) que se encuentra en la interfaz gráfica de usuario para la configuración de Flow Analysis pueden establecerse los atributos siguientes para la sonda de Flow Analysis:

Siga estos pasos:

1. Introduzca un nombre de usuario y una contraseña para el administrador de DSA para que Flow Analysis Collector pueda realizar la autenticación mediante el sistema del recopilador. De esta manera tendrá acceso al recurso compartido del recopilador.

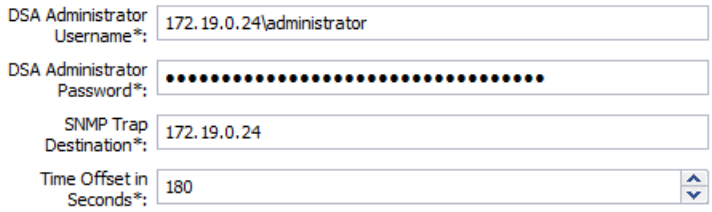
   Nota importante: El nombre de usuario del administrador de DSA es un nombre de usuario de Windows que tiene privilegios administrativos en el sistema del recopilador. Si otro usuario ha configurado el sistema del recopilador, consulte el nombre de usuario del administrador de DSA, que se ha configurado manualmente durante la configuración de Flow Analysis Collector, al administrador del servidor.

2. Introduzca el destino del mensaje SNMP, que es la dirección IP del robot que controla las sondas Flow Analysis y snmptd en el sistema del recopilador.

3. Modifique, si lo desea, el desplazamiento de tiempo en segundos (el valor predeterminado es 180 segundos). Mediante este retraso, las consultas a la base de datos se realizan poco tiempo después del inicio del nuevo período de intervalo de datos, evitando las incidencias de temporización causadas por la latencia de la base de datos. Generalmente, cuanto más rápido es el sistema del recopilador, más corto es el intervalo (y viceversa).

4. Reinicie el sistema del recopilador para crear una instancia de los cambios.

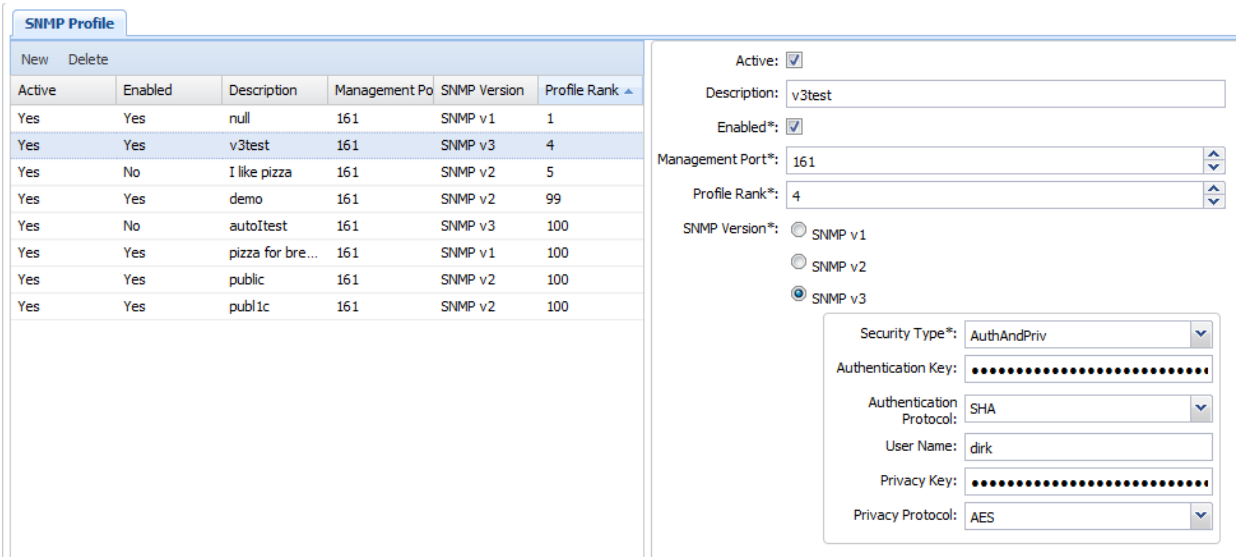
Nota: Los cambios realizados en la configuración se aplican al recopilador seleccionado en ese momento en el menú de la barra superior de la interfaz gráfica de usuario para la generación de informes de Flow Analysis.



Atributo	Tipo	Notas
DSA Administrator Username (Nombre de usuario del administrador de DSA)	Dirección IP\cadena	Ejemplo: 172.19.0.24\nqadmin (valor predeterminado)
DSA Administrator Password (Contraseña del administrador de DSA)	Cadena	Ejemplo: "nq" (valor predeterminado)
SNMP Trap Destination (Destino del mensaje SNMP)	Dirección IP	IP de snmptd (robot)
Time offset in Seconds (Desplazamiento de tiempo en segundos)	Número entero > 0	Valor predeterminado = 180

Configuración de los perfiles SNMP

Cuando se hace clic en **All Routers** (Todos los enrutadores) en el marco de la izquierda se muestra la pantalla **SNMP Profile** (Perfil de SNMP) en el marco de la derecha:

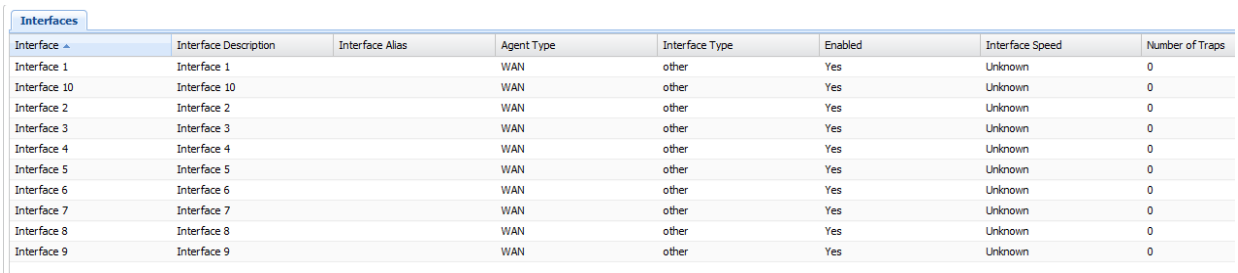


Cuando se hace clic en el elemento del menú **New** (Nuevo) en el perfil SNMP, o cuando se hace clic y se selecciona un perfil existente, se muestra, a la derecha, la interfaz gráfica de usuario para la configuración del **perfil SNMP**. Establezca los atributos siguientes mediante esta interfaz gráfica de usuario:

Atributo	**Tipo**	**Notas**
Active (Activo)	Booleano	Indica si el perfil se utiliza para el dispositivo seleccionado. El valor Active (Activo) es el valor predeterminado.
Enabled (Activado)	Booleano	Indica si el perfil se utiliza al intentar comunicarse con un dispositivo seleccionado. El valor Enabled (Activado) es el valor predeterminado.
Profile Rank (Clasificación del perfil)	Número entero	Muestra el orden en el cual se buscan coincidencias en el enrutador. Los números más bajos indican los valores iniciales en orden.
Management Port (Puerto de gestión)	Número entero	Valor predeterminado = 161
Description (Descripción)	Cadena	
SNMP Version (Versión de SNMP)	SNMP v1, v2 o v3	Establece la cadena de comunidad para SNMP v1 y v2.
		Para SNMP v3, establece el tipo de seguridad, la clave de autenticación, el protocolo de autenticación (ninguno, MD5 o SHA), el nombre de usuario, la clave de privacidad y el protocolo de privacidad (ninguno, DES, AES o Triple DES).

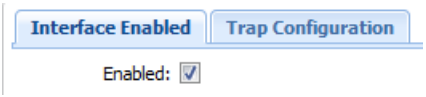
Configuración de las interfaces

Cuando se hace clic en un dispositivo de red de la lista del marco de la izquierda, se muestran las **interfaces** que están disponibles en el dispositivo de red seleccionado:


Interfaces

Interface	Interface Description	Interface Alias	Agent Type	Interface Type	Enabled	Interface Speed	Number of Traps
Interface 1	Interface 1		WAN	other	Yes	Unknown	0
Interface 10	Interface 10		WAN	other	Yes	Unknown	0
Interface 2	Interface 2		WAN	other	Yes	Unknown	0
Interface 3	Interface 3		WAN	other	Yes	Unknown	0
Interface 4	Interface 4		WAN	other	Yes	Unknown	0
Interface 5	Interface 5		WAN	other	Yes	Unknown	0
Interface 6	Interface 6		WAN	other	Yes	Unknown	0
Interface 7	Interface 7		WAN	other	Yes	Unknown	0
Interface 8	Interface 8		WAN	other	Yes	Unknown	0
Interface 9	Interface 9		WAN	other	Yes	Unknown	0

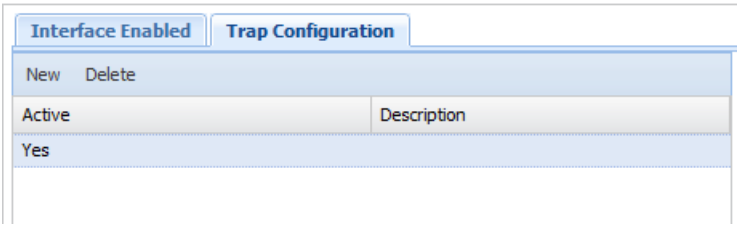
Cuando se hace clic en una interfaz, se muestra la interfaz gráfica de usuario para la configuración de la **interfaz activada** que se detalla a continuación:



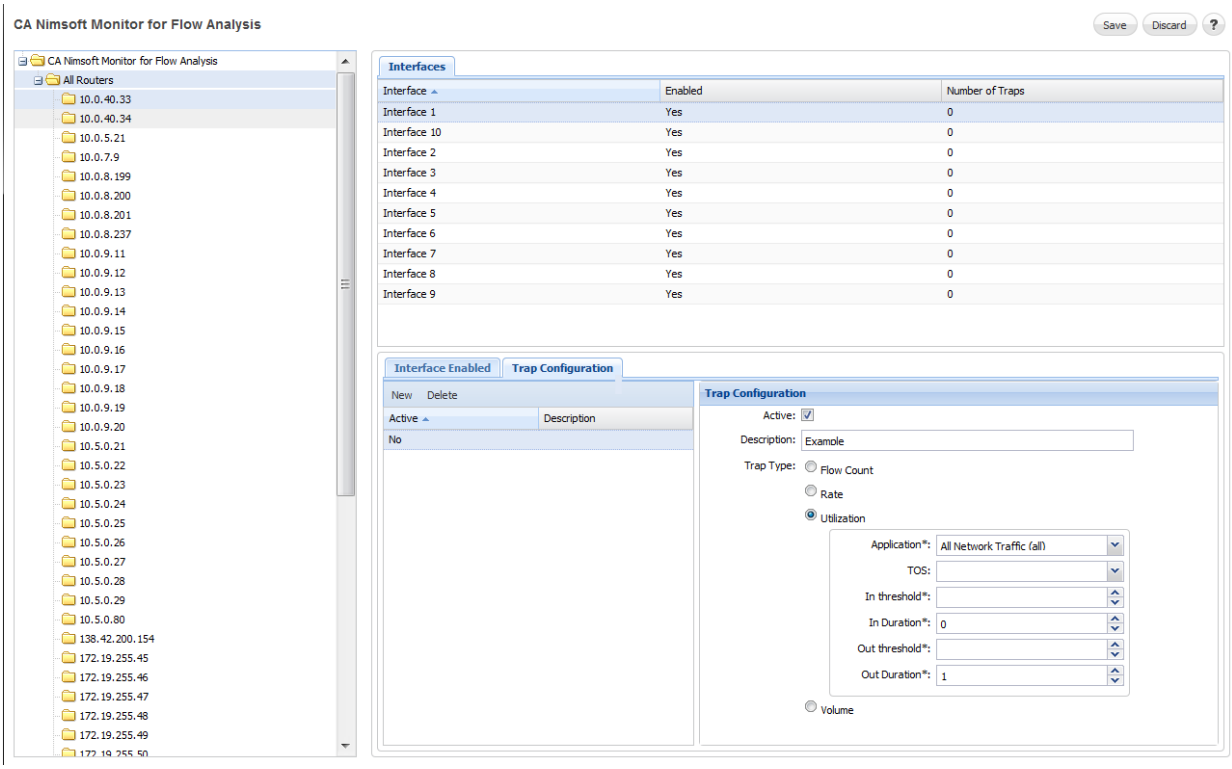
Atributo	Tipo	Notas
Enabled (Activado)	Booleano	Muestra si se está monitorizando la interfaz para los datos de NetFlow. El valor predeterminado es Enabled (Activado).

Configuración de los mensajes SNMP

Cuando se hace clic en **Trap Configuration** (Configuración de los mensajes SNMP), se muestra un listado de los mensajes SNMP definidos en una interfaz determinada del dispositivo de red seleccionado:



Cuando se hace clic en la configuración de un mensaje SNMP de la lista, a la derecha se muestra la interfaz gráfica de usuario para la **configuración del mensaje SNMP**:

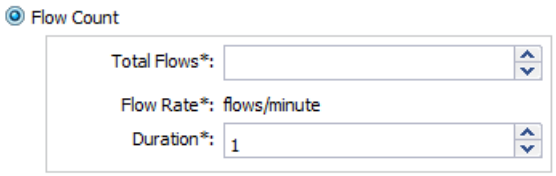


Todos los tipos de mensaje SNMP comparten dos atributos: Active (Activo) y Description (Descripción).

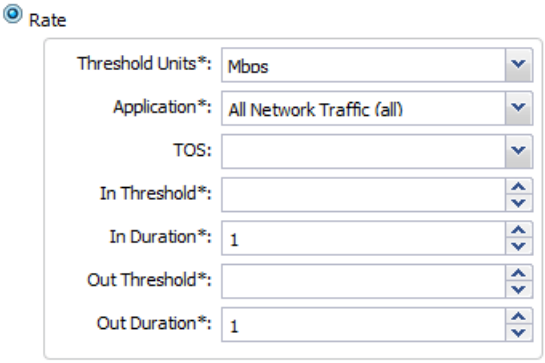
Atributo	Tipo	Notas
Active (Activo)	Booleano	Muestra si se utilizará un mensaje SNMP para la configuración especificada y la interfaz asignada. El valor predeterminado es Active (Activo).
Description (Descripción)	Cadena	

Cada tipo de mensaje SNMP ofrece atributos de configuración adicionales específicos según su finalidad:

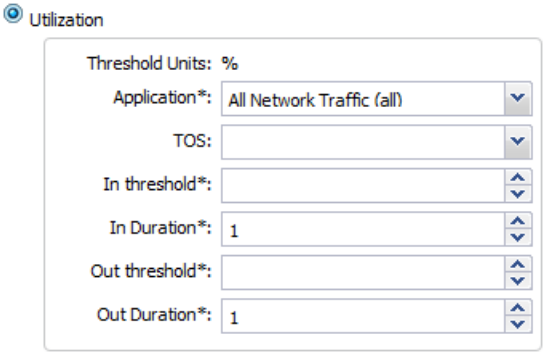
Flow Count (Recuento de flujos)



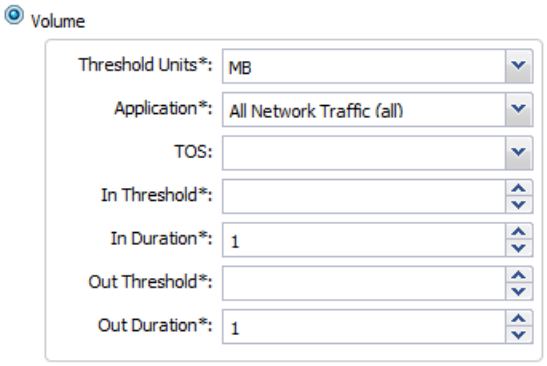
Rate (Clasificación)



Utilization (Utilización)



Volume (Volumen)



Configuración de los informes

Una vez realizados los pasos de configuración anteriores, se pueden visualizar los informes de Flow Analysis.

Consulte la sección Informes (en la página 29) para obtener información acerca de la configuración y la utilización de los informes de Flow Analysis y de las opciones disponibles.

Capítulo 3: Informes

Generación de informes de datos de Flow Analysis

La interfaz Web de Flow Analysis proporciona una vista integrada de las aplicaciones, los host y las interfaces de dispositivo principales de la red. Esta sección describe los tipos de informes y las opciones que están disponibles.

Flow Analysis ofrece una vista de varias dimensiones en los datos de flujo recibidos de la infraestructura de red. Se pueden cruzar los datos para contestar a estas o a otro tipo de preguntas:

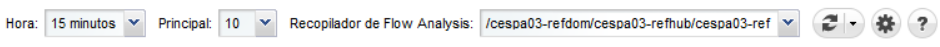
- ¿Quién ha hablado con quién? ¿Cuándo? (Optimización de las adjudicaciones y de los costes del ancho de banda o detección del tráfico malicioso)
- ¿Qué protocolo se utiliza con más frecuencia? (Optimización de los tipos de ofertas de servicio)
- ¿Dónde está el mayor volumen del tráfico de red? (Optimización de los valores de configuración de VPN y de la adjudicación de la banda ancha; solución de problemas originados por cambios repentinos en el uso)
- ¿Qué tipo de servicio (p. ej.: platino, oro, plata) se ve afectado?

El uso compartido de informes de flujo y datos de la calidad del servicio de UMP permite visualizar el entorno de servicio de las TI desde una perspectiva específica de un dispositivo, servicio o aplicación.

Elementos comunes

Los elementos de la interfaz gráfica de usuario siguientes están disponibles en todos los informes del portlet Flow Analysis:

Elementos de la barra superior



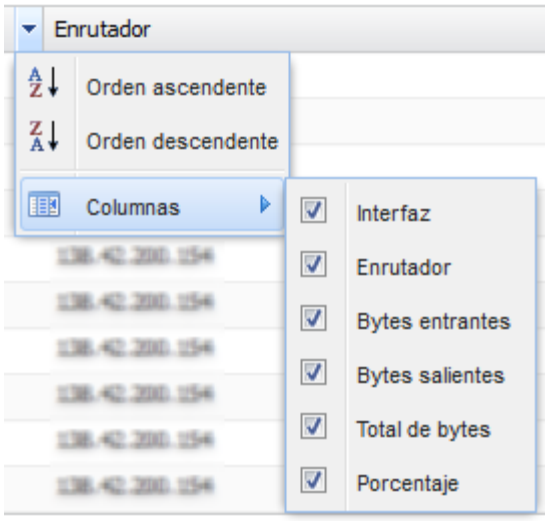
1. Time (Tiempo): Indica el intervalo de tiempo en el cual se han recopilado los datos mostrados. Los valores disponibles son: latest 15 min (últimos 15 minutos) (valor predeterminado), latest 1 hour (última hora), latest 4 hours (últimas 4 horas), latest day (último día), latest week (última semana).
2. Top (Principal): Indica el número de interfaces, host o aplicaciones que se muestran en los informes X principales (5, 10 (valor predeterminado), 15, 20 o 25).
3. Flow Analysis Collector (Recopilador de Flow Analysis): Muestra el recopilador que proporciona los datos a los informes. También se conoce como la sonda de Flow Analysis.
4. Botón de actualización: Realiza una consulta a la base de datos para obtener los últimos datos del intervalo. La actualización se puede realizar de forma manual o puede configurarse una actualización automática con intervalos de 1, 5, 10, o 15 minutos.
5. Botón de configuración: Abre el panel de configuración.
6. Botón de ayuda: Muestra la ayuda en línea.

Opciones para el gráfico

1. Gráfico de columnas
2. Gráfico de barras
3. Gráfico de líneas
4. Exportar a CSV. Haga clic en el icono e introduzca una ubicación para guardar. Se guardarán los datos que figuran en el informe.

Opciones para la vista de columna

Cuando se hace clic en un encabezado de columna se muestran los datos en orden ascendente o descendente. Se pueden ocultar o mostrar las columnas mediante las casillas de verificación.

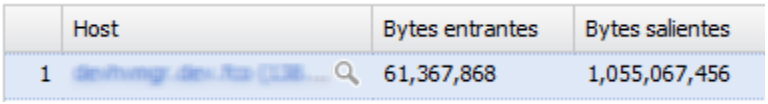


Arrastre de columnas

Se pueden arrastrar las columnas enteras en un orden preferido. Esta reclasificación de las columnas no es permanente, por lo que se restablece el orden predeterminado al actualizar o cerrar el explorador.

Vínculos para la obtención de detalles

Haga clic en los vínculos azules de las interfaces, host, conversaciones y otros elementos. Cada vista en UMP es una dirección URL profunda que si se copia y se pega en otra ventana del explorador o ficha muestra el mismo informe o la misma página Web con los datos actualizados procedentes del último intervalo de tiempo.



Visualización de la información sobre herramientas

Cuando se coloca el cursor encima de un elemento del informe, muestra información detallada sobre este. Cuando se pasa el cursor por la barra de datos del gráfico se obtiene información sobre las herramientas y se resaltan los datos correspondientes en la tabla. Sin embargo cuando se pasa por encima de una fila de datos de una tabla se resalta la barra del gráfico correspondiente.

Cadena de información

En la parte inferior derecha de cada gráfico de informe aparece el título que contiene los detalles sobre los datos que se muestran en el informe.

Ventana principal

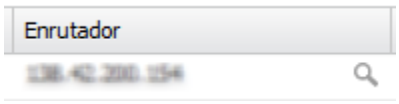
La ventana principal de Flow Analysis (que se muestra en la imagen siguiente) muestra los datos X principales para los flujos de datos entre:

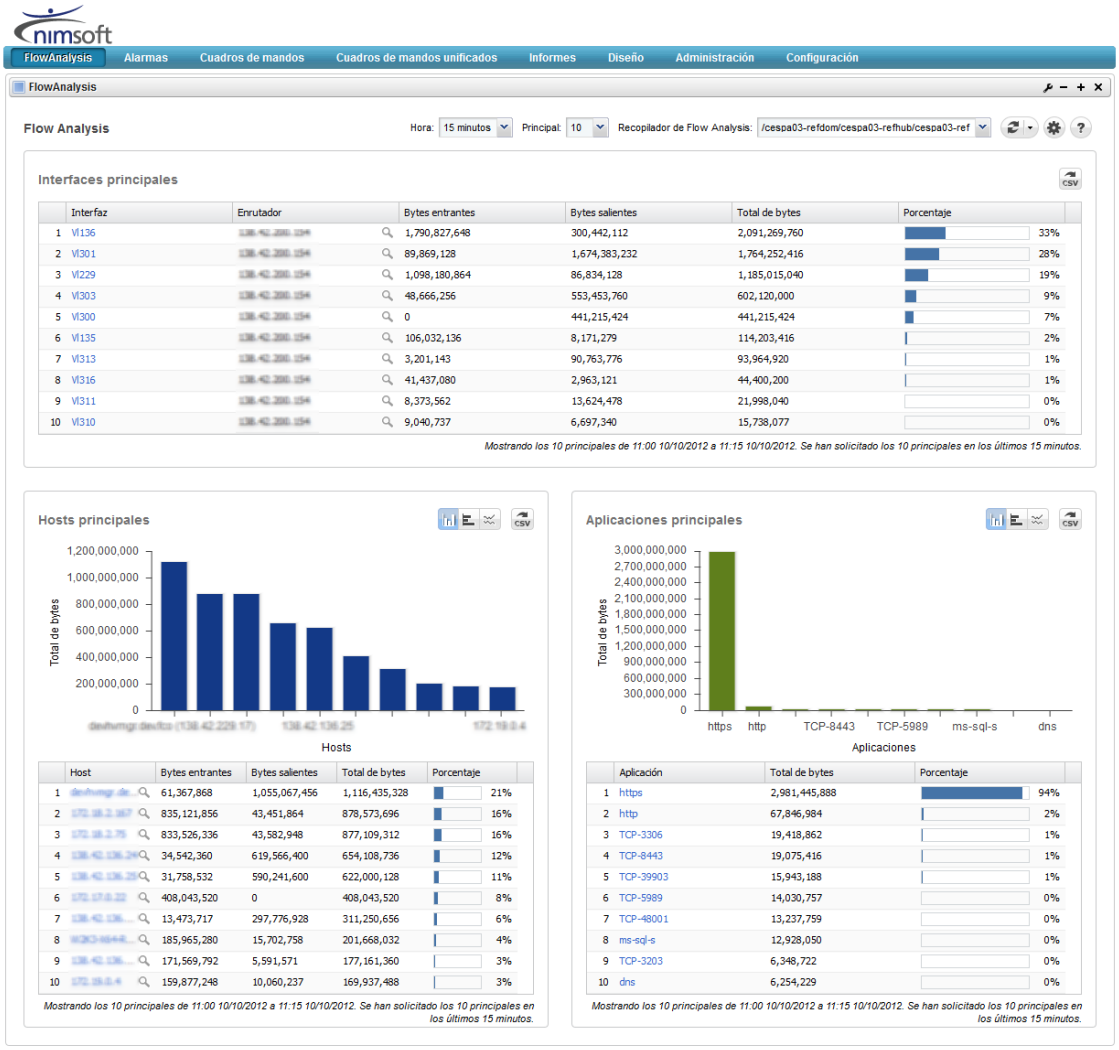
- Interfaces principales
- Host principales
- Aplicaciones principales (protocolos)

Cuando se hace clic en un nombre de interfaz en la gráfica de las interfaces más utilizadas se muestra un informe detallado de las conversaciones, los host y las aplicaciones principales desde la perspectiva de la interfaz.

De forma similar, cuando se hace clic en un nombre de host o de aplicación en la gráfica correspondiente, se muestran los detalles del host o de la aplicación y se proporciona información adicional.

Haga clic en el vínculo USM para buscar el dispositivo del Gestor de servicios unificados (solamente se proporciona información adicional para algunos dispositivos):



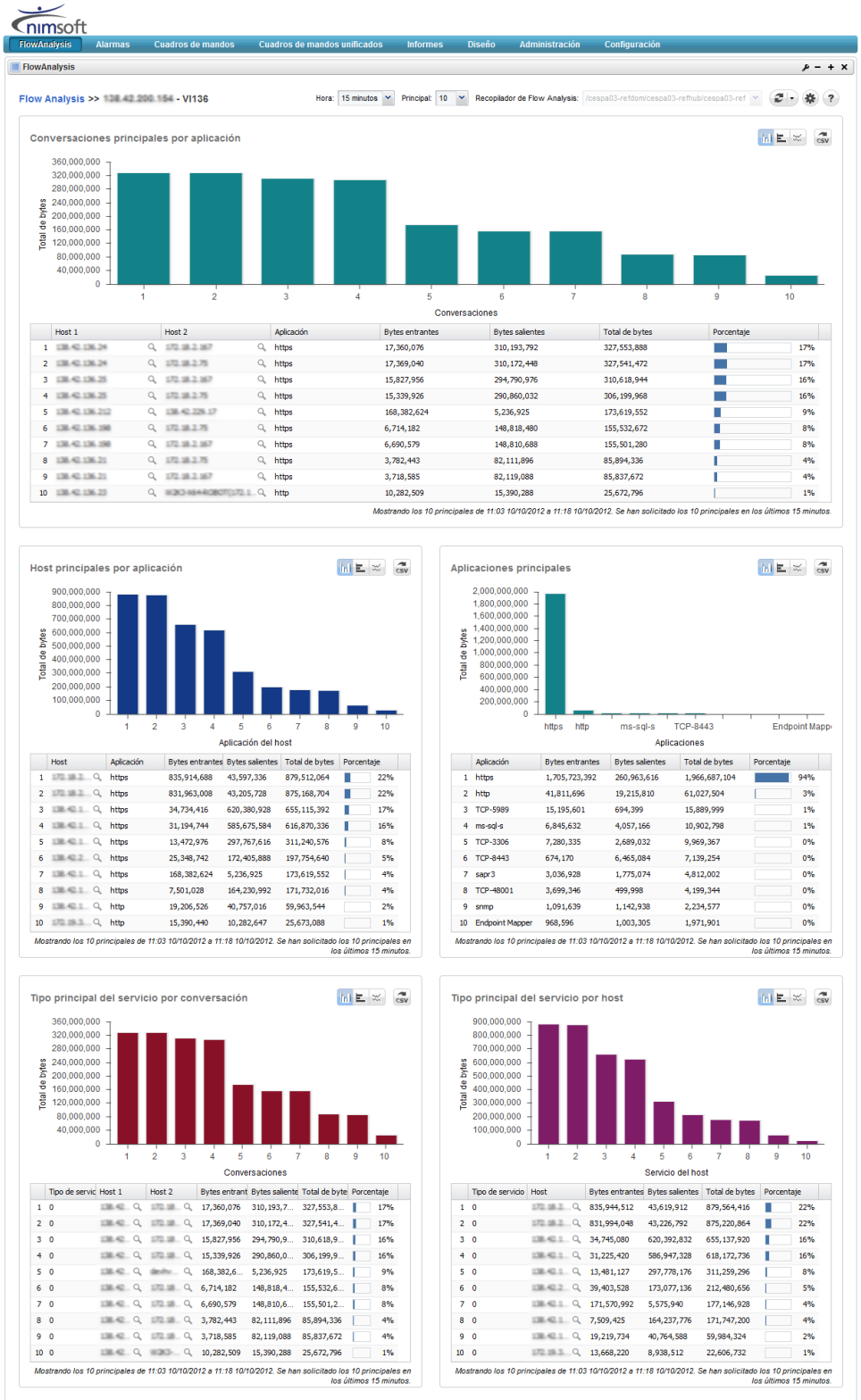

nimsoft
FlowAnalysis
Alarmas
Cuadros de mandos
Cuadros de mandos unificados
Informes
Diseño
Administración
Configuración
FlowAnalysis
Flow Analysis
Hora: 15 minutos
Principal: 10
Recopilador de Flow Analysis: /cespa03-refdom/cespa03-refhub/cespa03-ref
Interfaces principales
CSV
Interfaz
Enrutador
Bytes entrantes
Bytes salientes
Total de bytes
Porcentaje
1 Vl136 1,790,827,648 300,442,112 2,091,269,760 33%
2 Vl301 89,869,128 1,674,383,232 1,764,252,416 28%
3 Vl229 1,098,180,864 86,834,128 1,185,015,040 19%
4 Vl303 48,666,256 553,453,760 602,120,000 9%
5 Vl300 0 441,215,424 441,215,424 7%
6 Vl135 106,032,136 8,171,279 114,203,416 2%
7 Vl313 3,201,143 90,763,776 93,964,920 1%
8 Vl316 41,437,080 2,963,121 44,400,200 1%
9 Vl311 8,373,562 13,624,478 21,998,040 0%
10 Vl310 9,040,737 6,697,340 15,738,077 0%
Mostrando los 10 principales de 11:00 10/10/2012 a 11:15 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Hosts principales
CSV
1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
0
Total de bytes
Hosts
Host
Bytes entrantes
Bytes salientes
Total de bytes
Porcentaje
1 61,367,868 1,055,067,456 1,116,435,328 21%
2 835,121,856 43,451,864 878,573,696 16%
3 833,526,336 43,582,948 877,109,312 16%
4 34,542,360 619,566,400 654,108,736 12%
5 31,758,532 590,241,600 622,000,128 11%
6 408,043,520 0 408,043,520 8%
7 13,473,717 297,776,928 311,250,656 6%
8 185,965,280 15,702,758 201,668,032 4%
9 171,569,792 5,591,571 177,161,360 3%
10 159,877,248 10,060,237 169,937,488 3%
Mostrando los 10 principales de 11:00 10/10/2012 a 11:15 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Aplicaciones principales
CSV
3,000,000,000
2,700,000,000
2,400,000,000
2,100,000,000
1,800,000,000
1,500,000,000
1,200,000,000
900,000,000
600,000,000
300,000,000
0
Total de bytes
https
http
TCP-8443
TCP-5989
ms-sql-s
dns
Aplicaciones
Aplicación
Total de bytes
Porcentaje
1 https 2,981,445,888 94%
2 http 67,846,984 2%
3 TCP-3306 19,418,862 1%
4 TCP-8443 19,075,416 1%
5 TCP-39903 15,943,188 1%
6 TCP-5989 14,030,757 0%
7 TCP-48001 13,237,759 0%
8 ms-sql-s 12,928,050 0%
9 TCP-3203 6,348,722 0%
10 dns 6,254,229 0%
Mostrando los 10 principales de 11:00 10/10/2012 a 11:15 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.

Interfaces

Cuando en un informe principal se accede a los detalles de una interfaz, se muestra el tráfico que está fluyendo a través de la interfaz del dispositivo de red seleccionada. Estos informes muestran:

- Conversaciones principales por aplicación
- Hosts principales por aplicación
- Aplicaciones principales
- Tipo principal del servicio por conversación
- Tipo principal del servicio por host

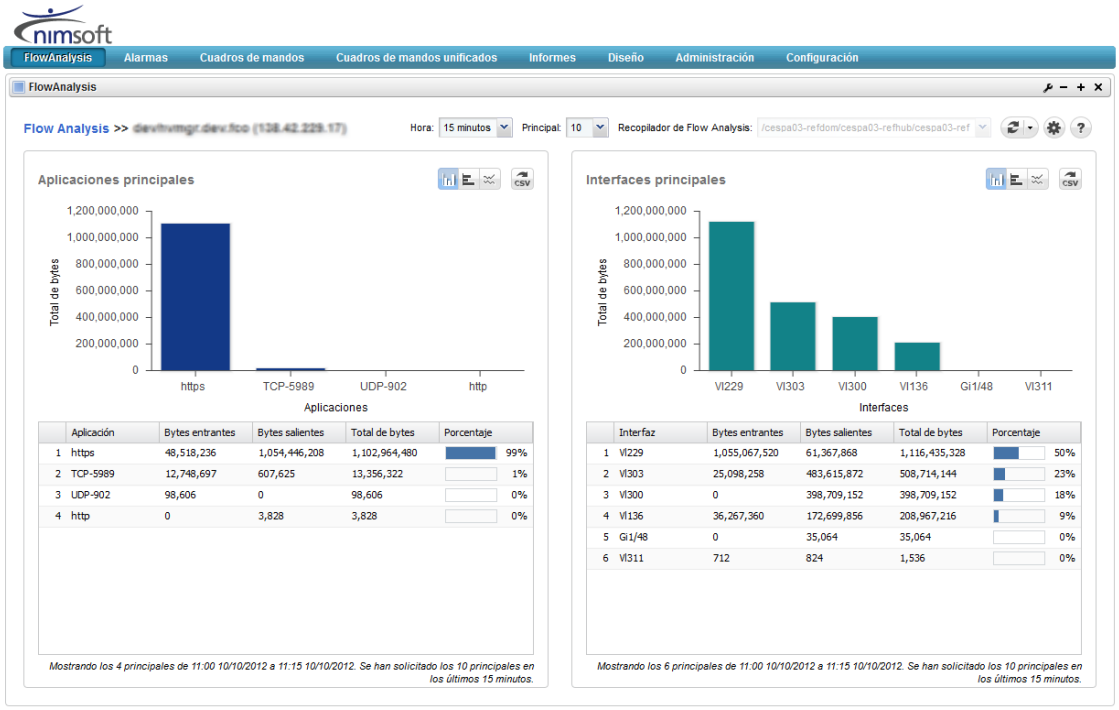
Esta información resulta útil cuando se optimizan los valores de configuración de VPN y la adjudicación de la banda ancha, se mejoran las ofertas de servicio o se solucionan los problemas originados por cambios repentinos en el uso. Se puede utilizar para optimizar las adjudicaciones de la banda ancha o para detectar el tráfico malicioso.


nimsoft
FlowAnalysis
Alarmas
Cuadros de mandos
Cuadros de mandos unificados
Informes
Diseño
Administración
Configuración
FlowAnalysis
Flow Analysis >> [redacted] - VI136
Hora: 15 minutos
Principal: 10
Recopilador de Flow Analysis: /cespa03-refdom/cespa03-refhub/cespa03-ref
Conversaciones principales por aplicación
Total de bytes
Conversaciones
Host 1 | Host 2 | Aplicación | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 | [redacted] | [redacted] | https | 17,360,076 | 310,193,792 | 327,553,888 | 17%
2 | [redacted] | [redacted] | https | 17,369,040 | 310,172,448 | 327,541,472 | 17%
3 | [redacted] | [redacted] | https | 15,827,956 | 294,790,976 | 310,618,944 | 16%
4 | [redacted] | [redacted] | https | 15,339,926 | 290,860,032 | 306,199,968 | 16%
5 | [redacted] | [redacted] | https | 168,382,624 | 5,236,925 | 173,619,552 | 9%
6 | [redacted] | [redacted] | https | 6,714,182 | 148,818,480 | 155,532,672 | 8%
7 | [redacted] | [redacted] | https | 6,690,579 | 148,810,688 | 155,501,280 | 8%
8 | [redacted] | [redacted] | https | 3,782,443 | 82,111,896 | 85,894,336 | 4%
9 | [redacted] | [redacted] | https | 3,718,585 | 82,119,088 | 85,837,672 | 4%
10 | [redacted] | [redacted] | http | 10,282,509 | 15,390,288 | 25,672,796 | 1%
Mostrando los 10 principales de 11:03 10/10/2012 a 11:18 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Host principales por aplicación
Total de bytes
Aplicación del host
Host | Aplicación | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 | [redacted] | https | 835,914,688 | 43,597,336 | 879,512,064 | 22%
2 | [redacted] | https | 831,963,008 | 43,205,728 | 875,168,704 | 22%
3 | [redacted] | https | 34,734,416 | 620,380,928 | 655,115,392 | 17%
4 | [redacted] | https | 31,194,744 | 585,675,584 | 616,870,336 | 16%
5 | [redacted] | https | 13,472,976 | 297,767,616 | 311,240,576 | 8%
6 | [redacted] | https | 25,348,742 | 172,405,888 | 197,754,640 | 5%
7 | [redacted] | https | 168,382,624 | 5,236,925 | 173,619,552 | 4%
8 | [redacted] | https | 7,501,028 | 164,230,992 | 171,732,016 | 4%
9 | [redacted] | http | 19,206,526 | 40,757,016 | 59,963,544 | 2%
10 | [redacted] | http | 15,390,440 | 10,282,647 | 25,673,088 | 1%
Mostrando los 10 principales de 11:03 10/10/2012 a 11:18 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Aplicaciones principales
Total de bytes
https
http
ms-sql-s
TCP-8443
Endpoint Mapp
Aplicaciones
Aplicación | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 | https | 1,705,723,392 | 260,963,616 | 1,966,687,104 | 94%
2 | http | 41,811,696 | 19,215,810 | 61,027,504 | 3%
3 | TCP-5989 | 15,195,601 | 694,399 | 15,889,999 | 1%
4 | ms-sql-s | 6,845,632 | 4,057,166 | 10,902,798 | 1%
5 | TCP-3306 | 7,280,335 | 2,689,032 | 9,969,367 | 0%
6 | TCP-8443 | 674,170 | 6,465,084 | 7,139,254 | 0%
7 | sapr3 | 3,036,928 | 1,775,074 | 4,812,002 | 0%
8 | TCP-48001 | 3,699,346 | 499,998 | 4,199,344 | 0%
9 | snmp | 1,091,639 | 1,142,938 | 2,234,577 | 0%
10 | Endpoint Mapper | 968,596 | 1,003,305 | 1,971,901 | 0%
Mostrando los 10 principales de 11:03 10/10/2012 a 11:18 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Tipo principal del servicio por conversación
Total de bytes
Conversaciones
Tipo de servic | Host 1 | Host 2 | Bytes entrant | Bytes saliente | Total de byte | Porcentaje
1 | 0 | [redacted] | [redacted] | 17,360,076 | 310,193,7... | 327,553,8... | 17%
2 | 0 | [redacted] | [redacted] | 17,369,040 | 310,172,4... | 327,541,4... | 17%
3 | 0 | [redacted] | [redacted] | 15,827,956 | 294,790,9... | 310,618,9... | 16%
4 | 0 | [redacted] | [redacted] | 15,339,926 | 290,860,0... | 306,199,9... | 16%
5 | 0 | [redacted] | [redacted] | 168,382,6... | 5,236,925 | 173,619,5... | 9%
6 | 0 | [redacted] | [redacted] | 6,714,182 | 148,818,4... | 155,532,6... | 8%
7 | 0 | [redacted] | [redacted] | 6,690,579 | 148,810,6... | 155,501,2... | 8%
8 | 0 | [redacted] | [redacted] | 3,782,443 | 82,111,896 | 85,894,336 | 4%
9 | 0 | [redacted] | [redacted] | 3,718,585 | 82,119,088 | 85,837,672 | 4%
10 | 0 | [redacted] | [redacted] | 10,282,509 | 15,390,288 | 25,672,796 | 1%
Mostrando los 10 principales de 11:03 10/10/2012 a 11:18 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Tipo principal del servicio por host
Total de bytes
Servicio del host
Tipo de servicio | Host | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 | 0 | [redacted] | 835,944,512 | 43,619,912 | 879,564,416 | 22%
2 | 0 | [redacted] | 831,994,048 | 43,226,792 | 875,220,864 | 22%
3 | 0 | [redacted] | 34,745,080 | 620,392,832 | 655,137,920 | 16%
4 | 0 | [redacted] | 31,225,420 | 586,947,328 | 618,172,736 | 16%
5 | 0 | [redacted] | 13,481,127 | 297,778,176 | 311,259,296 | 8%
6 | 0 | [redacted] | 39,403,528 | 173,077,136 | 212,480,656 | 5%
7 | 0 | [redacted] | 171,570,992 | 5,575,940 | 177,146,928 | 4%
8 | 0 | [redacted] | 7,509,425 | 164,237,776 | 171,747,200 | 4%
9 | 0 | [redacted] | 19,219,734 | 40,764,588 | 59,984,324 | 2%
10 | 0 | [redacted] | 13,668,220 | 8,938,512 | 22,606,732 | 1%
Mostrando los 10 principales de 11:03 10/10/2012 a 11:18 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.

Hosts

En la ventana principal, cuando se accede a los detalles de un host, se muestran dos informes sobre su tráfico:

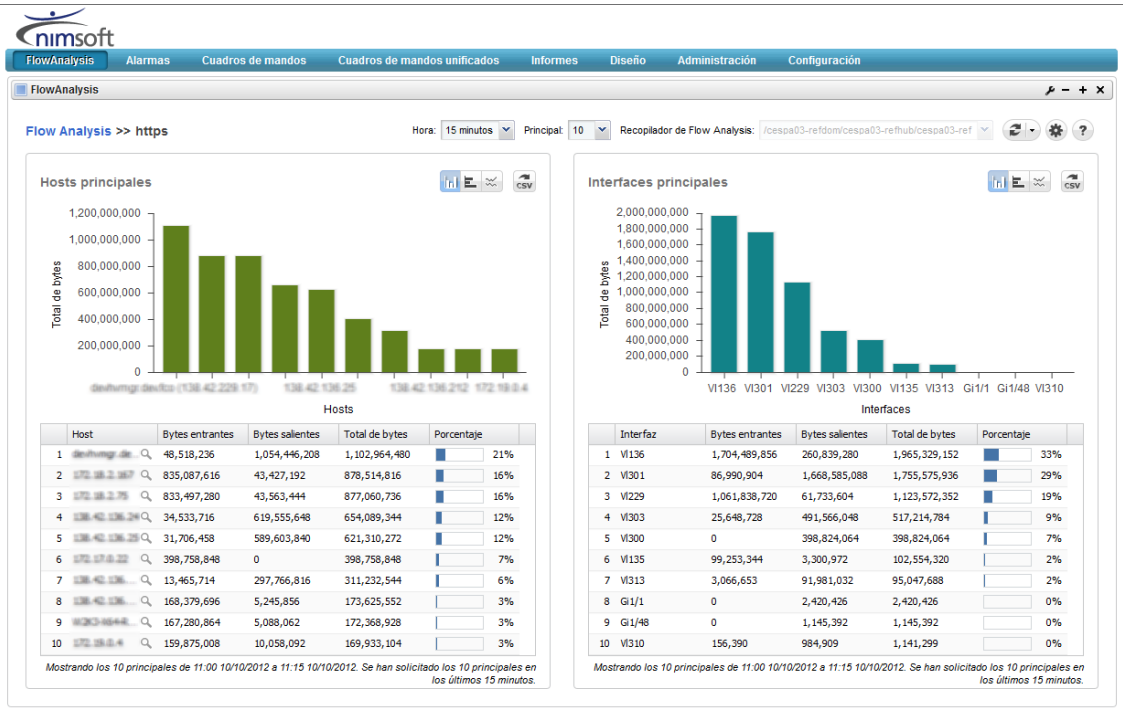
- Aplicaciones principales
- Interfaces principales


nimsoft
FlowAnalysis
Alarmas
Cuadros de mandos
Cuadros de mandos unificados
Informes
Diseño
Administración
Configuración
FlowAnalysis
Flow Analysis >>
Hora: 15 minutos
Principal: 10
Recopilador de Flow Analysis:
Aplicaciones principales
Total de bytes
1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
0
https
TCP-5989
UDP-902
http
Aplicaciones
Aplicación | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 https | 48,518,236 | 1,054,446,208 | 1,102,964,480 | 99%
2 TCP-5989 | 12,748,697 | 607,625 | 13,356,322 | 1%
3 UDP-902 | 98,606 | 0 | 98,606 | 0%
4 http | 0 | 3,828 | 3,828 | 0%
Mostrando los 4 principales de 11:00 10/10/2012 a 11:15 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.
Interfaces principales
Total de bytes
1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
0
Vl229
Vl303
Vl300
Vl136
Gi1/48
Vl311
Interfaces
Interfaz | Bytes entrantes | Bytes salientes | Total de bytes | Porcentaje
1 Vl229 | 1,055,067,520 | 61,367,868 | 1,116,435,328 | 50%
2 Vl303 | 25,098,258 | 483,615,872 | 508,714,144 | 23%
3 Vl300 | 0 | 398,709,152 | 398,709,152 | 18%
4 Vl136 | 36,267,360 | 172,699,856 | 208,967,216 | 9%
5 Gi1/48 | 0 | 35,064 | 35,064 | 0%
6 Vl311 | 712 | 824 | 1,536 | 0%
Mostrando los 6 principales de 11:00 10/10/2012 a 11:15 10/10/2012. Se han solicitado los 10 principales en los últimos 15 minutos.

Aplicación

Cuando se accede a los detalles de una aplicación desde la pantalla principal, en función del protocolo, se muestran hasta dos informes de detalles:

- Host principales
- Interfaces principales



Capítulo 4: Solución de problemas

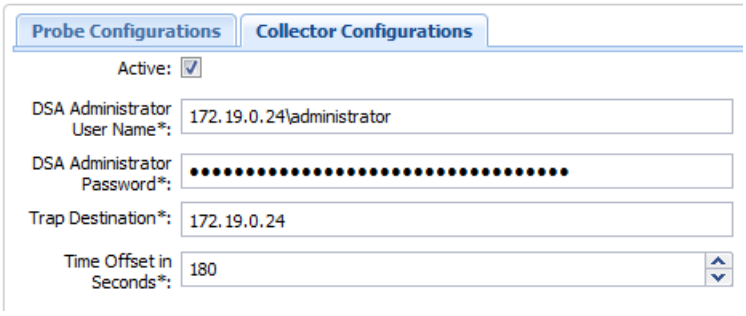
No se muestran datos en los informes (retraso del tiempo de los datos del informe)

Válido en todas las plataformas

Síntoma: Se muestra el mensaje de error siguiente:

No se han devuelto datos
Es posible que no haya datos dentro del marco de tiempo especificado. Si espera ver datos en el marco de tiempo especificado, pruebe las sugerencias siguientes:
Haga clic aquí para volver a intentarlo.
Compruebe el estado de monitoring_services.
Compruebe que la sonda de flow para el recopilador Flow Analysis "/cespa03-refdom/cespa03-refhub/cespa03-ref" está ejecutándose y funciona correctamente.
Detalles:
Código de estado de HTTP: 204 No Content

Solución: Configure el valor de configuración Time Offset (Desplazamiento de tiempo) en la ficha Collector Configurations (Configuraciones del recopilador).



Es posible que en sistemas lentos de Flow Analysis Collector sea necesario establecer un valor mayor para el valor de configuración **Time Offset in Seconds** (Desplazamiento de tiempo en segundos).

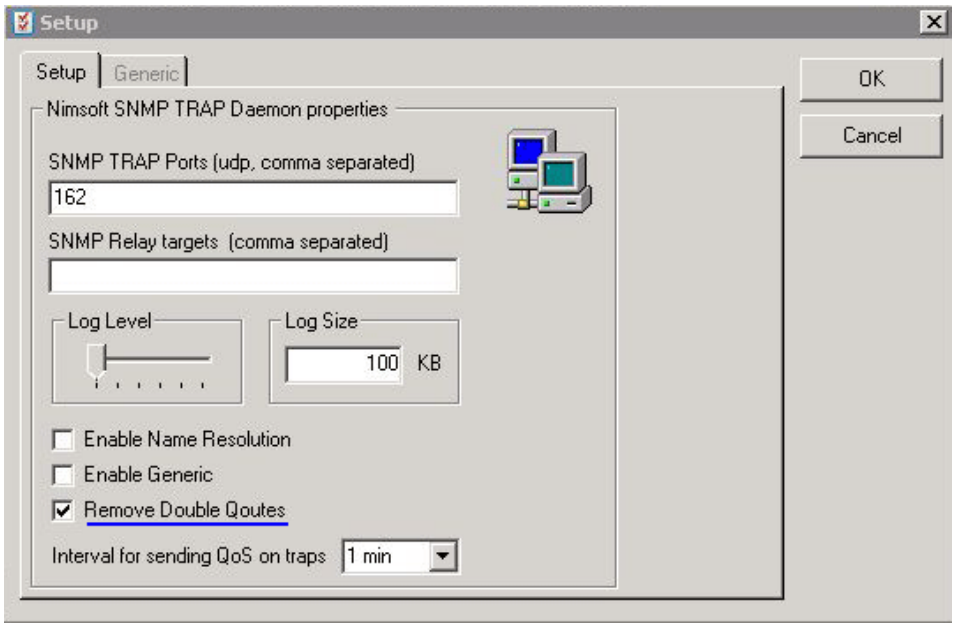
No funcionan los vínculos a USM

Válido en todas las plataformas

Síntoma: Después de hacer clic en el icono de la lupa para la búsqueda de USM en la interfaz gráfica de usuario de Flow Analysis, el sistema muestra el mensaje "No hay ninguna métrica disponible". Esto sucede para todos los dispositivos que se buscan en USM.

Solución: Verifique que la sonda snmptd está configurada correctamente realice lo siguiente:

En la configuración de la sonda snmptd, haga doble clic en el icono de la sonda snmptd en el Gestor de la infraestructura y asegúrese de que está marcada la casilla de verificación Remove Double Quotes (Eliminar comillas dobles).



El vínculo a USM muestra un dispositivo incorrecto

Válido en todas las plataformas

Síntoma: Después de hacer clic en el icono de la lupa para la búsqueda de USM en la interfaz gráfica de usuario de Flow Analysis, se redirige al dispositivo incorrecto en la vista de USM.

Motivo: Si un dispositivo no está configurado como parte de un grupo de USM, el algoritmo de búsqueda de USM no puede encontrar ninguna coincidencia exacta y devuelve la coincidencia más cercana que encuentra.

Solución: Compruebe en UMP si el dispositivo está configurado en un grupo. Si no está en un grupo, agréguelo a un grupo existente o cree un nuevo grupo y agréguelo al nuevo grupo.

No se muestra el recopilador en el menú desplegable

Válido en todas las plataformas

Síntoma: Cuando se hace clic en la barra superior del menú desplegable para mostrar los recopiladores disponibles, no se muestra ningún recopilador o el recopilador deseado no aparece en la lista.

Motivo: Los servicios de detección no encuentran la sonda Collector en el sistema del recopilador.

Solución: Detenga y reinicie las sondas Discovery_server y Discovery_agent desde el Gestor de la infraestructura.

Interfaz denominada Null0 o Nu0

Válido en todas las plataformas

Síntoma: Una de las interfaces X principales se muestra con el nombre en blanco.

Motivo: El comportamiento del dispositivo de Cisco predeterminado es asignar datos de flujo para tráfico incorrecto en el dispositivo a una interfaz falsa denominada Null0 o Nu0. Si la interfaz Nu0 de un enrutador aparece en un informe de flujo, el nombre de la interfaz se muestra en blanco.

Solución: No existe ninguna solución. Se trata de un comportamiento esperado.

Código de mensaje de error 500

Síntoma: Aparece el código de error 500.

Causa: Los servicios de monitorización no pueden encontrar ninguna sonda. Este hecho puede significar que no se esté ejecutando la sonda discovery_server. Aunque la sonda no se esté ejecutando, aparece marcada en naranja o rojo en la lista de detección.

Código de mensaje de error 400

Síntoma: Aparece el código de error 400.

Causa: No se puede establecer comunicación con la sonda. Esto sucede cuando la sonda no se está ejecutando o no se puede establecer comunicación con ella.

Código de mensaje de error 200

Síntoma: Aparece el código de error 200.

Causa: La sonda responde con un conjunto de datos vacío. Es posible que suceda cuando no haya datos disponibles para el intervalo de tiempo seleccionado o cuando la hora del sistema establecida en el cuadro de NetQoS sea inexacta.